REMARKS

Claims 17-21, 26-27, and 33-40 are pending in this application, of which claims 17, 33, and 37-40 are amended herein. Claims 37-40 are amended merely to correct typographical errors. No new matter has been introduced. In view of the following remarks, reconsideration and allowance of the application is respectfully requested.

Claims 17-21 and 26-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Albert et al. (US Patent Application Publication 2003/0177389). However, Applicants respectfully submit that Albert fails to teach, disclose, or render obvious each and every feature of claims 17-21 and 26-27.

Claim 17 recites, in relevant part, a method for securing a computer system that includes one or more mobile devices located on a user's side of a network connection and a computing node located on a network side of the network connection, comprising executing a node security program in the computing node for interpreting a node security profile, determining at least one security parameter from the interpretation of the node security profile, managing, from the network side of the network connection, at least one security process between the computing node and one or more mobile devices based on the at least one security parameter determined by interpreting the node security profile, and transferring a device security profile to a mobile device or a resource device to be interpreted by a device security program running on the mobile device to determine device security parameters.

Thus, as is recited in claim 17, the computing node is located on the network side of the network connection between the computing node and the one or more mobile devices. The Examiner's attention is respectfully directed to paragraphs [0041]-[0044] of the present specification for a more detailed description of the computing node of the invention. For example, when a mobile device connects to the network that includes the computing node, the method recited in claim 17 enables the computing node to manage, from the network side of the network connection, at least one security process between the computing node and one or more mobile devices, and to verify that the right security policies are enforced on the mobile device.

In contrast, Albert relates generally to a series of methods that allow a mobile device to apply a security policy required for connection to a particular network (i.e. an end-point security system that formalizes the interaction from a user client-side device of policies required by the user for his device). For example, Albert relates to end-point (client device) security in which the client device is augmented with security software that acquires up-to-date policies from the Integrity Policy Server. Based on the network the device is connecting to, the on-device security software merges various on-device policies to create the right device policies that must be enforced to properly connect with the target network. In addition, Albert specifically discloses methods "enabling a user to have more than one security policy active at the same time on his or her computing device," and that the invention "enables a user to comply with a plurality of different security policies which may be required from time to time as the user connects to different networks and resources." (See paragraph [0047]). Thus, Albert addresses the network security problem of connecting PCs, Laptops, and Mobile Devices to various networks that have different security requirements. (See paragraph [0009]). There is no suggestion whatsoever in Albert to use a computing node located on the network side of the network connection between the computing node and one or more mobile devices to verify, from the network side of the network connection, that the right security policies are enforced on the mobile device, as is recited in claim 17. In addition, Albert fails to disclose managing, from the network side of the network connection, at least one security process between the computing node and one or more mobile devices based on the at least one security parameter determined by interpreting the node security profile, as is recited in claim 17.

Accordingly, as Albert fails to disclose each and every element of claim 17, Applicants respectfully request that the rejection of claim 17 under 35 U.S.C. § 102(e) be reconsidered and withdrawn. Dependent claims 18-21 and 26-27 are allowable based on their dependency on claim 17, and also on their own merits.

Claims 33-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Albert in view of Sharma et al (US Patent Application Publication 2002/0068559). However, Applicants respectfully submit that neither Albert nor Sharma, taken alone or in combination, disclose, suggest, or render obvious the invention as recited in claims 33-40.

Claim 33 recites, in relevant part, a method for managing a computer system including a computing node located on a network side of a network connection and one or more mobile devices located on a user's side of the network connection, comprising running a discovery program to detect one or more mobile devices or resources, determining information regarding one or more mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource, and using the determined mobile device information to manage security of the computer system from the network side of the network connection.

As is described above, the computing node of the invention is located on the network side of the network connection between the computing node and the one or more mobile devices, and Albert fails to disclose the use of a computing node located on the network side of the network connection between the computing node and one or more mobile devices. Moreover, Albert fails to disclose managing, from the network side of the network connection, security of the computer system from the network side of the network connection.

Sharma fails to overcome the deficiencies of Albert described above. In addition, Sharma fails to disclose or suggest running a discovery program to detect one or more mobile devices or resources. Moreover, Sharma fails to disclose using determined mobile device information to manage security of the computer system from the network side of the network connection. Instead, Sharma relates to the use of mobile devices in the management of network assets on a network. (See, for example, paragraph [0010]). There is no suggestion whatsoever in either Sharma or Albert that the mobile devices themselves may be discovered through the execution of a discovery program, as is recited in claim 33. Moreover, there is no suggestion whatsoever in either Sharma or Albert that determined mobile device information may be used to manage the security of a computer system from the network side of the network connection, as is recited in claim 33.

Therefore, neither Albert nor Sharma, taken alone or in combination, disclose, suggest, or render obvious each and every element of claim 33. Thus, Applicants respectfully request that the rejection of claim 33 under 35 U.S.C. § 103(a) be reconsidered and withdrawn. Dependent claims 34-40 are allowable based on their dependency on claim 33, and also on their own merits.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

Respectfully submitted,

NIXON PEABODY, LLP

Date: September 28, 2006

/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler

NIXON PEABODY LLP
Customer No. 22204
401 9th Street, N.W., Suite 900
Washington, D.C. 20004
(202) 585-8000